Exhibit 19

https://learn.microsoft.com/en-us/legal/cognitive-services/openai/code-of-conduct?context=%2Fazure%2Fai-services%2Fopenai%2Fcontext%2Fcontext

Microsoft Generative AI Services Code of Conduct

Article • 07/30/2024

This Code of Conduct defines the requirements that all customers of Microsoft Generative AI Services (as defined in the Microsoft Product Terms , and including Azure OpenAI Service) and Azure AI Content Safety must adhere to in good faith. These requirements apply in addition to the Microsoft Product Terms, including the Acceptable Use Policy.

Responsible AI mitigation requirements

Customers must ensure that all of their applications built with Microsoft Generative AI Services and Azure AI Content Safety:

- Implement meaningful human oversight.
- Implement technical and operational measures to detect fraudulent user behavior in account creation and during use.
- Implement strong technical limits on inputs and outputs to reduce the likelihood of misuse beyond the application's intended purpose.
- Disclose the synthetic nature of generated voices, images, and/or videos to users such that users are not likely to be deceived or duped – or able to prank others – into believing they are interacting with a real person or that any voice or other generated content is authentic or attributable to a specific individual.
- Test applications thoroughly to find and mitigate undesirable behaviors
- Establish feedback channels.
- Implement additional scenario-specific mitigations as appropriate.

To learn more, see the Responsible AI transparency documentation for the applicable Microsoft Generative AI Service, for example, the Azure OpenAI Transparency Note and the Azure AI Content Safety Transparency Note.

Usage restrictions

Customers, users, and applications built with Microsoft Generative AI Services and Azure AI Content Safety must NOT use the services:

- In any way that is inconsistent with this Code of Conduct, including the Responsible AI mitigation requirements, the Content requirements, and any applicable Limited Access Requirements;
- To interact with individuals under the age of consent in any way that could result in exploitation or manipulation or is otherwise prohibited by law or regulation;
- To generate or interact with content prohibited in this Code of Conduct;
- To present content alongside or to monetize content prohibited in this Code of Conduct;
- To make decisions without appropriate human oversight as part of an application that may have a consequential impact on any individual's legal position, financial position, life opportunities, employment opportunities, or human rights, or may result in physical or psychological harm to an individual;
- To deploy subliminal techniques (e.g., visual, auditory, or other signals beyond a normal person's range of perception) with the intent to deceive or cause harm;
- To deceive or intentionally misinform, for false advertising, or to manipulate or distort the behavior of a person in a way that causes harm
- To exploit any of the vulnerabilities of a person (e.g., age, disability, or socio-economic situation);
- For social scoring or predictive profiling that would lead to discriminatory, unfair, biased, detrimental, unfavorable, or harmful treatment of certain persons or groups of persons;
- To categorize people based on their biometric data or to infer characteristics or affiliations about them such as race, political opinions, trade union membership, religious or philosophical beliefs, or sex life or sexual orientation;
- To infer people's sensitive attributes such as gender, race, nationality, religion, or specific age (not including age range, position of mouth (e.g., smile or frown) , and hair color);
- To attempt to infer people's emotional states from their physical, physiological, or behavioral characteristics (e.g., facial expressions, facial movements, or speech patterns), including inferring emotions such as anger, disgust, happiness, sadness, surprise, fear, or other terms commonly used to describe a person's emotional state;
- For chatbots that (i) are erotic, romantic, or used for erotic or romantic purposes, or which are otherwise prohibited by this Code of Conduct; (ii) are personas of specific people without their explicit consent; (iii) claim to have special wisdom/insight/knowledge, unless very clearly labeled as being for entertainment purposes only; or (iv) enable end users to create their own chatbots without oversight;
- Except for customers approved for modified content filtering, to identify or verify individual identities based on people's faces, voices, or other physical, physiological,

or behavioral characteristics;

- For unlawful tracking, stalking, or harassment of a person;
- Without the individual's valid consent, for ongoing surveillance or real-time or near real-time identification or persistent tracking of the individual using any of their personal information, including biometric data;
- For facial recognition purposes (including identification or verification of individual identities) by or for a state or local police department in the United States;
- For any real-time facial recognition technology on mobile cameras used by any law enforcement globally to attempt to identify individuals in uncontrolled, "in the wild" environments, which includes (without limitation) police officers on patrol using body-worn or dash-mounted cameras using facial recognition technology to attempt to identify individuals present in a database of suspects or prior inmates;
- To generate content with the purpose of removing or altering content credentials or other provenance methods, marks, or signals ("AI Content Credentials") that indicate that the content was generated by a Microsoft Generative AI Service;
- To generate content with the purpose of misleading others about whether the content was generated by a Microsoft Generative AI Service; or
- To detect AI Content Credentials with the purpose of removing or altering them.

Content requirements

Microsoft prohibits the use of Microsoft Generative AI Services for processing, generating, classifying, or filtering content in ways that can inflict harm on individuals or society. Our content policies are intended to improve the safety of our services and how they are used.

These content requirements apply to use of features of, and the output of, all Microsoft Generative AI Services and Azure AI Content Safety. This includes, but is not limited to, use of features of Azure OpenAI Service and all content provided as input to or generated as output from all models available in Azure OpenAI Service, such as GPT-3, GPT-4, GPT-4 Turbo with Vision, Codex models, DALL·E 2, DALL·E 3, and Whisper. These requirements apply to the use of Azure AI Content Safety, including features such as customized categories, and to all content provided as input to the service and content generated as output from the service regardless of content filter settings.

Exploitation and abuse

Child sexual exploitation and abuse

Microsoft prohibits content that describes, features, or promotes child sexual exploitation or abuse, whether or not prohibited by law. This includes sexual content involving a child or that sexualizes a child.

Grooming

Microsoft prohibits content that describes or is used for purposes of grooming of children. Grooming is the act of an adult building a relationship with a child for the purposes of exploitation, especially sexual exploitation. This includes communicating with a child for the purpose of sexual exploitation, trafficking, or other forms of exploitation.

Non-consensual intimate content

Microsoft prohibits content that describes, features, or promotes non-consensual intimate activity.

Sexual solicitation

Microsoft prohibits content that describes, features, or promotes, or is used for, purposes of solicitation of commercial sexual activity and sexual services. This includes encouragement and coordination of real sexual activity.

Trafficking

Microsoft prohibits content describing or used for purposes of human trafficking. This includes the recruitment of individuals, facilitation of transport, and payment for, and the promotion of, exploitation of people such as forced labor, domestic servitude, sexual slavery, forced marriages, and forced medical procedures.

Sexually explicit content

Microsoft prohibits the creation of erotic, pornographic, or otherwise sexually explicit content. This includes sexually suggestive content, depictions of sexual activity, and fetish content.

Suicide and self-injury

Microsoft prohibits content that describes, praises, supports, promotes, glorifies, encourages and/or instructs individual(s) on self-injury or to take their life.

Violent content and conduct

Graphic violence and gore

Microsoft prohibits content that describes, features, or promotes graphic violence or gore.

Terrorism and violent extremism

Microsoft prohibits content that depicts an act of terrorism; praises, or supports a terrorist organization, terrorist actor, or violent terrorist ideology; encourages terrorist activities; offers aid to terrorist organizations or terrorist causes; or aids in recruitment to a terrorist organization.

Violent threats, incitement, and glorification of violence

Microsoft prohibits content advocating or promoting violence toward others through violent threats or incitement.

Harmful content

Hate speech and discrimination

Microsoft prohibits content that attacks, denigrates, intimidates, degrades, targets, or excludes individuals or groups on the basis of traits such as actual or perceived race, ethnicity, national origin, gender, gender identity, sexual orientation, religious affiliation, age, disability status, caste, or any other characteristic that is associated with systemic prejudice or marginalization.

Bullying and harassment

Microsoft prohibits content that targets individual(s) or group(s) with threats, intimidation, insults, degrading or demeaning language or images, promotion of physical harm, or other abusive behavior such as stalking.

Deception, disinformation, and inauthentic activity

Microsoft prohibits content that is intentionally deceptive and likely to adversely affect the public interest, including deceptive or untrue content relating to health, safety, election integrity, or civic participation. Microsoft also prohibits inauthentic interactions, such as fake accounts, automated inauthentic activity, impersonation to gain unauthorized information or privileges, and claims to be from any person, company, government body, or entity without explicit permission to make that representation.

Active malware or exploits

Content that supports unlawful active attacks or malware campaigns that cause technical harms, such as delivering malicious executables, organizing denial of service attacks, or managing command and control servers.

Additional content policies

Microsoft prohibits the use of Microsoft Generative AI Services for scenarios in which the AI system is likely to generate undesired content due to limitations in the models or scenarios in which the system cannot be applied in a way that properly manages potential negative consequences to people and society. Without limiting the foregoing restriction, Microsoft reserves the right to revise and expand the above Content requirements to address specific harms to people and society.

Microsoft may at times limit our services' ability to respond to particular topics, such as probing for personal information or seeking opinions on sensitive topics or current events, even if not prohibited by this Code of Conduct.

Microsoft prohibits the use of Microsoft Generative AI Services for activities that significantly harm other individuals, organizations, or society, including but not limited to use of the service for purposes in conflict with the applicable Azure Legal Terms and the Microsoft Product Terms.

Transmitting harmful content to Azure AI Content Safety through the intended use of the service will not by itself be considered a violation of this Code of Conduct. However, Azure AI Content Safety must not be used to collect harmful content based on the above categories, or to classify, collect, or filter content in a way that would violate the other sections of this Code of Conduct, except as provided in the Limited Exception below.

Limited exception

Customers are permitted to provide, generate, classify, collect, and filter content in ways that would otherwise violate this Code of Conduct solely (1) to evaluate, train, and improve safety systems and applications for Customer's use to the extent permitted by the Microsoft Product Terms and (2) to evaluate and test Microsoft Generative AI Services to the extent permitted by the Penetration Testing Rules of Engagement . Customers may use any resulting harmful content solely for evaluation and reporting and not for any other purpose. Customers remain responsible for all legal compliance relating to such content, including without limitation, retention, destruction, and reporting as necessary.

Report abuse

If you suspect that a Microsoft Generative AI Service is being used in a manner that is abusive or illegal, infringes on your rights or the rights of other people, or violates these policies, you can report it at the Report Abuse Portal.

See also

- Limited access to Azure OpenAI Service
- Overview of Responsible AI practices
- Transparency note for Azure OpenAI Service
- Data, privacy, and security for Azure OpenAI Service